Car Fob Hacking

Security experts say that the best way to store your car keys at night is by putting them in a coffee can, but guess what an ex-FBI agent's advice is to protect cars from theft during the day? **Wrapping car fobs in aluminum foil?** "Although it's not ideal, it is the most inexpensive way," said Holly Hubert, a cybersecurity expert who retired in 2017 from the FBI in Buffalo, New York. "The cyber threat is so dynamic and ever changing, it's hard for consumers to keep up." She suggests clients go online and spend a few dollars and buy what's called a

Faraday bag to shield the fob signal from potential theft. Imagine a traditional sandwich bag made of foil instead of plastic.

But why? Thing is, the car is always waiting for the fob signal. Thieves can buy legitimate devices that amplify the fob signal sitting unprotected in a purse, a pocket, on a counter at home or even just copy the code to access the vehicle. The cheap (or homemade) metal protection covers, named for the scientist who figured out how to block an electromagnetic field, can prevent thieves from having access to vehicles with a wireless fob. Currently, thieves can capture fob signals from outside a home, office or hotel room.

Some people say they use credit card holders to protect their key fob, but these don't work because they're essentially a net rather than a wall. Clifford Neuman, director of the University of Southern California Center for Computer Systems Security in Los Angeles, pointed to the millions of consumers who now carry their credit cards in a protective pocket designed to work as a Faraday cage, but these credit card pockets are not that effective at protecting car fobs since you need to block the fob's signal from going out, not just protect it from being scanned, which is how a credit car protector works. A bad actor can go up to a house with a car parked in front of it, use a very inexpensive device to detect a fob 10 feet away in a bedroom, and use the fob's signal to unlock and start the car to drive away in it. A very quick and easy method for car thieves. As these devices become more available, this scenario becomes more and more likely.

Cars used to be hot-wired and that was the common type of car theft, but this technique required physically breaking into the car, which was a risky and timely process, But the high value of vehicles made this an accepted risk. Hijacking your car fob's signal is becoming the go to technique used by criminals. How much you are concerned, and what you do about it, is a matter of your risk management. People who store their fobs in Faraday cages, or just aluminum foil, aren't paranoid, rather they are exercising caution in a digital world full of unknown dangers, so why not?

This is the reality of a wireless, connected world where car doors lock with a click and a chirp, where children in the back seat stream videos and companies can update software technology remotely. While auto industry engineers know a lot

about traditional safety, quality, compliance and reliability challenges, cyber is an adaptive adversary. Automakers are starting to implement security features in every stage of design and manufacturing, including the key fob. But the bad guys seem to always be one step ahead of the good guys, so protecting yourself is not paranoid.

Thank you for subscribing to our email!